

CLAIMS

1. A record carrier comprising:

a storage unit;

5 a requisition receiving unit operable to receive, from
a terminal device having the record carrier attached thereto,
a requisition for access to the storage unit;

an acquisition unit operable to acquire an access
condition indicating whether or not the terminal device is
10 authorized to access the storage unit;

a judging unit operable to judge whether or not the
requisition satisfies the access condition; and

a prevention unit operable to prevent the access of the
terminal device to the storage unit when the judging unit judges
15 that the requisition does not satisfy the access condition.

2. The record carrier of Claim 1, further comprising:

an access condition storage unit operable to store the access
condition, wherein

20 the acquisition unit acquires the access condition from the
access condition storage unit.

3. The record carrier of Claim 2, wherein

the access condition includes an identifier list including

one or more identifiers which respectively identify one or more devices authorized to access the storage unit,

the requisition includes a requiring device identifier for identifying the terminal device, and

5 the judging unit judges that, (i) when an identifier matching the requiring device identifier is included in the identifier list, the requisition satisfies the access condition, and (ii) when an identifier matching the requiring device identifier is not included in the identifier list, the requisition does not satisfy the access
10 condition.

4. The record carrier of Claim 2, wherein

the access condition includes an identifier list including one or more identifiers and one or more sets of number information
15 which correspond one-to-one with the identifiers respectively, the one or more identifiers identifying one or more devices authorized to access the storage unit, each set of number information indicating a count of accesses available for the corresponding device to access the storage unit,

20 the requisition includes a requiring device identifier for identifying the terminal device,

the judging unit includes:

a holding unit operable to hold a count of accesses indicating how many times the terminal device has accessed the
25 storage unit;

a 1st judging subunit operable to judge whether or not

an identifier matching the requiring device identifier is included in the identifier list; and

5 a 2nd judging subunit operable to judge, when the 1st judging subunit judges that the matching identifier is included, whether or not a count indicated by a set of number information corresponding to the matching identifier is larger than the count of accesses held by the holding unit, and

the judging unit judges that, (i) when either one of a judgment result by the 1st judging subunit and a judgment result
10 by the 2nd judging subunit is negative, the requisition does not satisfy the access condition, and (ii) when both the judgment results are positive, the requisition satisfies the access condition.

15 5. The record carrier of Claim 2, wherein

the access condition includes an identifier list including one or more identifiers and one or more sets of period information which correspond one-to-one with the identifiers respectively, the one or more identifiers identifying one or more devices authorized
20 to access the storage unit, each set of period information indicating a time period available for the corresponding device to access the storage unit,

the requisition includes a requiring device identifier for identifying the terminal device, and

25 the judging unit includes:

a time managing unit operable to manage a current date

and time;

a 1st judging subunit operable to judge whether or not an identifier matching the requiring device identifier is included in the identifier list; and

5 a 2nd judging subunit operable to judge, when the 1st judging subunit judges that the matching identifier is included, whether or not the current time is within a time period indicated by a set of period information corresponding to the matching identifier, and

10 the judging unit judges that, (i) when either one of a judgment result by the 1st judging subunit and a judgment result by the 2nd judging subunit is negative, the requisition does not satisfy the access condition, and (ii) when both the judgment results are positive, the requisition satisfies the access
15 condition.

6. The record carrier of Claim 2, wherein

the storage unit includes a plurality of memory blocks,
the access condition includes an identifier list including
20 one or more identifiers and one or more sets of memory block information, which correspond one-to-one with the identifiers respectively identifying one or more devices authorized to access the storage unit, the sets of memory block information each indicating one or more of the memory blocks available for each of
25 the corresponding devices to access,

the requisition includes a requiring device identifier for

identifying the terminal device and memory block specifying information for specifying one of the memory blocks, and

the judging unit includes:

5 a 1st judging subunit operable to judge whether or not an identifier matching the requiring device identifier is included in the identifier list; and

10 a 2nd judging subunit operable to judge, when the 1st judging subunit judges that the matching identifier is included, whether or not the memory block specified by the memory block specifying information is included in the one or more of the memory blocks indicated by a set of the memory block information corresponding to the matching identifier, and

15 the judging unit judges that, (i) when either one of a judgment result by the 1st judging subunit and a judgment result by the 2nd judging subunit is negative, the requisition does not satisfy the access condition, and (ii) when both the judgment results are positive, the requisition satisfies the access condition.

20 7. The record carrier of Claim 2, wherein

the storage unit stores one or more sets of program data, the access condition includes an identifier list including one or more identifiers and one or more sets of program information, which correspond one-to-one with the identifiers respectively
25 identifying one or more devices authorized to access the storage unit, the sets of program information each indicating one or more

sets of the program data available for each of the corresponding devices to access,

the requisition includes a requiring device identifier for identifying the terminal device and program specifying
5 information for specifying one set of the program data, and

the judging unit includes:

a 1st judging subunit operable to judge whether or not an identifier matching the requiring device identifier is included in the identifier list; and

10 a 2nd judging subunit operable to judge, when the 1st judging subunit judges that the matching identifier is included, whether or not the set of program data specified by the program specifying information is included in the one or more sets of the program data indicated by a set of the program information
15 corresponding to the matching identifier, and

the judging unit judges that, (i) when either one of a judgment result by the 1st judging subunit and a judgment result by the 2nd judging subunit is negative, the requisition does not satisfy the access condition, and (ii) when both the judgment
20 results are positive, the requisition satisfies the access condition.

8. The record carrier of Claim 2, wherein

the access condition includes (i) an identifier list
25 including one or more identifiers which respectively identify one or more devices authorized to access the storage unit, and (ii)

a biometrics list including one or more sets of biometric information for respectively identifying one or more users authorized to access the storage unit,

the requisition includes a requiring device identifier for
5 identifying the terminal device and operator biometric information indicating biometric information of an operator of the terminal device, and

the judging unit includes:

a 1st judging subunit operable to judge whether or not
10 an identifier matching the requiring device identifier is included in the identifier list; and

a 2nd judging subunit operable to judge, when the 1st judging subunit judges that the matching identifier is included, whether or not a set of the biometric information corresponding
15 to the operator biometric information is included in the biometrics list, and

the judging unit judges that, (i) when either one of a judgment result by the 1st judging subunit and a judgment result by the 2nd judging subunit is negative, the requisition does not
20 satisfy the access condition, and (ii) when both the judgment results are positive, the requisition satisfies the access condition.

9. The record carrier of Claim 2, wherein

25 the access condition includes (i) an identifier list including one or more identifiers which respectively identify one

or more devices authorized to access the storage unit, and (ii) a password list including one or more sets of password information respectively specified by one or more users authorized to access the storage unit,

5 the requisition includes a requiring device identifier for identifying the terminal device and an entry password entered by an operator of the terminal device, and

the judging unit includes:

10 a 1st judging subunit operable to judge whether or not an identifier matching the requiring device identifier is included in the identifier list; and

a 2nd judging subunit operable to judge whether or not a password indicated by a set of password information corresponding to the entry password is included in the password list, and

15 the judging unit judges that, (i) when either one of a judgment result by the 1st judging subunit and a judgment result by the 2nd judging subunit is negative, the requisition does not satisfy the access condition, and (ii) when both the judgment results are positive, the requisition satisfies the access
20 condition.

10. The record carrier of Claim 2, further comprising:

25 an access condition accepting unit operable to accept the access condition from a terminal device having the record carrier attached thereto; and

an access condition registration unit operable to register,

when the terminal device is authorized, the access condition with the access condition storage unit.

11. The record carrier of Claim 10, wherein

5 the access condition registration unit includes:

a 1st key information holding unit holds 1st key information shared with the authorized terminal device; and

an output unit operable to output challenge data to the terminal device having the record carrier attached thereto; and

10 an examination unit operable to receive response data from the terminal device having the record carrier attached thereto and examine the received response data,

and the access condition registration unit authenticates that, when, as a result of the examination, the response data is
15 verified as data generated by using the challenge data and the 1st key information, the terminal device having the record carrier attached thereto is the authorized terminal device.

12. The record carrier of Claim 11, wherein

20 the access condition accepting unit accepts the access condition which has been encrypted using an access condition encryption key, and

the access condition registration unit decrypts the encrypted access condition based on the access condition encryption
25 key, and registers the decrypted access condition with the access condition storage unit.

13. The record carrier of Claim 12, wherein

the access condition accepting unit further accepts signature data generated based on the access condition, and

5 the access condition registration unit examines the signature data using a verification key relevant to the authorized terminal device, and registers, when the signature data is successfully verified, the decrypted access condition with the access condition storage unit.

10 14. The record carrier of Claim 13, wherein

the access condition includes an identifier list including one or more identifiers which respectively identify one or more devices authorized to access the storage unit.

15 15. The record carrier of Claim 13, wherein

the access condition includes an identifier list,

the identifier list comprises one or more identifiers and one or more sets of number information which correspond one-to-one
20 with the identifiers,

the one or more identifiers respectively identify one or more devices authorized to access the storage unit, and

each set of number information indicates a count of accesses available for the corresponding devices to access the storage unit.

25 16. The record carrier of Claim 13, wherein

the access condition includes an identifier list,

the identifier list comprises one or more identifiers and one or more sets of period information which correspond one-to-one with the identifiers,

5 the one or more identifiers respectively identify one or more devices authorized to access the storage unit, and

each set of period information respectively indicates a time period available for the corresponding device to access the storage unit.

10

17. The record carrier of Claim 13, wherein

the storage unit comprises a plurality of memory blocks,

the access condition includes an identifier list,

15 the identifier list comprises one or more identifiers and one or more sets of memory block information, which correspond one-to-one with the identifiers,

the identifiers respectively identify one or more devices authorized to access the storage unit, and

20 the sets of memory block information each indicate one or more of the memory blocks available for each of the corresponding devices to access.

18. The record carrier of Claim 13, wherein

the storage unit stores one or more sets of program data,

25 the access condition includes an identifier list,

the identifier list comprises one or more identifiers and

one or more sets of program information, which correspond one-to-one with the identifiers,

the identifiers respectively identify one or more devices authorized to access the storage unit, and

5 the sets of program information each indicate one or more sets of the program data available for each of the corresponding devices to access.

19. The record carrier of Claim 13, wherein

10 the access condition includes an identifier list and a biometrics list,

the identifier list comprises one or more identifiers respectively identifying one or more devices authorized to access the storage unit, and

15 the biometrics list comprises one or more sets of biometric information for respectively identifying one or more users authorized to access the storage unit.

20. The record carrier of Claim 13, wherein

20 the access condition includes an identifier list and a password list,

the identifier list comprises one or more identifiers respectively identifying one or more devices authorized to access the storage unit, and

25 the password list comprises one or more sets of password information respectively specified by one or more users authorized

to access the storage unit.

21. The record carrier of Claim 2, further comprising:

a deletion requisition receiving unit operable to receive,
5 from the terminal device having the record carrier attached thereto,
a requisition for deletion of the access condition stored by the
access condition storage unit,

an authentication unit operable to authenticate whether or
not the terminal device is authorized, and

10 an access condition deletion unit operable to delete, when
the authentication unit authenticates that the terminal device is
authorized, the access condition from the access condition storage
unit according to the requisition.

15 22. The record carrier of Claim 2, further comprising:

an update requisition receiving unit operable to receive,
from the terminal device having the record carrier attached thereto,
a requisition for update of the access condition stored by the access
condition storage unit,

20 an authentication unit operable to authenticate whether or
not the terminal device is authorized, and

an access condition update unit operable to update, when the
authentication unit authenticates that the terminal device is
authorized, the access condition according to the requisition.

25

23. The record carrier of Claim 1, further comprising:

a communication unit operable to communicate with an access condition management server connected via a network, wherein

the acquisition unit acquires the access condition from the access condition management server via the communication unit.

5

24. The record carrier of Claim 23,

wherein the acquisition unit acquires from the access condition management server via the communication unit, along with the access condition, signature data generated based on the access condition, and

10

the record carrier further comprising:

a tamper detection unit operable to examine the signature data using a verification key relevant to the access condition management server, and detect whether or not the access condition has been tampered; and

15

a prohibition unit operable to prohibit, when the tamper detection detects that the access condition has been tampered, the judging unit from judging

20 25. The record carrier of Claim 24, wherein

the access condition includes an identifier list including one or more identifiers which respectively identify one or more devices authorized to access the storage unit,

the requisition includes a requiring device identifier for identifying the terminal device, and

25

the judging unit judges that, (i) when an identifier matching

the requiring device identifier is included in the identifier list,
the requisition satisfies the access condition, and (ii) when an
identifier matching the requiring device identifier is not included
in the identifier list, the requisition does not satisfy the access
5 condition.

26. The record carrier of Claim 24, wherein

the access condition includes an identifier list including
one or more identifiers and one or more sets of number information
10 which correspond one-to-one with the identifiers respectively, the
one or more identifiers identifying one or more devices authorized
to access the storage unit, each set of number information
indicating a count of accesses available for the corresponding
device to access the storage unit,

15 the requisition includes a requiring device identifier for
identifying the terminal device,

the judging unit includes:

a holding unit operable to hold a count of accesses
indicating how many times the terminal device has accessed the
20 storage unit;

a 1st judging subunit operable to judge whether or not
an identifier matching the requiring device identifier is included
in the identifier list; and

a 2nd judging subunit operable to judge, when the 1st
25 judging subunit judges that the matching identifier is included,
whether or not a count indicated by a set of number information

corresponding to the matching identifier is larger than the count of accesses held by the holding unit, and

the judging unit judges that, (i) when either one of a judgment result by the 1st judging subunit and a judgment result by the 2nd judging subunit is negative, the requisition does not satisfy the access condition, and (ii) when both the judgment results are positive, the requisition satisfies the access condition.

27. The record carrier of Claim 24, wherein

the access condition includes an identifier list including one or more identifiers and one or more sets of period information which correspond one-to-one with the identifiers respectively, the one or more identifiers identifying one or more devices authorized to access the storage unit, each set of period information indicating a time period available for the corresponding device to access the storage unit,

the requisition includes a requiring device identifier for identifying the terminal device, and

the judging unit includes:

a time managing unit operable to manage a current date and time;

a 1st judging subunit operable to judge whether or not ~~an identifier matching the requiring device identifier~~ is included in the identifier list; and

a 2nd judging subunit operable to judge, when the 1st

judging subunit judges that the matching identifier is included, whether or not the current time is within a time period indicated by a set of period information corresponding to the matching identifier, and

5 the judging unit judges that, (i) when either one of a judgment result by the 1st judging subunit and a judgment result by the 2nd judging subunit is negative, the requisition does not satisfy the access condition, and (ii) when both the judgment results are positive, the requisition satisfies the access
10 condition.

28. The record carrier of Claim 24, wherein

the storage unit comprises a plurality of memory blocks,
the access condition includes an identifier list including
15 one or more identifiers and one or more sets of memory block information, which correspond one-to-one with the identifiers respectively identifying one or more devices authorized to access the storage unit, the sets of memory block information each indicating one or more of the memory blocks available for each of
20 the corresponding devices to access,

the requisition includes a requiring device identifier for identifying the terminal device and memory block specifying information for specifying one of the memory blocks, and

the judging unit includes:

25 a 1st judging subunit operable to judge whether or not an identifier matching the requiring device identifier is included

in the identifier list; and

a 2nd judging subunit operable to judge, when the 1st judging subunit judges that the matching identifier is included, whether or not the memory block specified by the memory block specifying information is included in the one or more of the memory blocks indicated by a set of the memory block information corresponding to the matching identifier,

and judges that, (i) when either one of a judgment result by the 1st judging subunit and a judgment result by the 2nd judging subunit is negative, the requisition does not satisfy the access condition, and (ii) when both the judgment results are positive, the requisition satisfies the access condition.

29. The record carrier of Claim 24, wherein

the storage unit stores one or more sets of program data, the access condition includes an identifier list including one or more identifiers and one or more sets of program information, which correspond one-to-one with the identifiers respectively identifying one or more devices authorized to access the storage unit, the sets of program information each indicating one or more sets of the program data available for each of the corresponding devices to access,

the requisition includes a requiring device identifier for identifying the terminal device and program specifying information for specifying one set of the program data, and

the judging unit includes:

a 1st judging subunit operable to judge whether or not an identifier matching the requiring device identifier is included in the identifier list; and

a 2nd judging subunit operable to judge, when the 1st judging subunit judges that the matching identifier is included, whether or not the set of program data specified by the program specifying information is included in the one or more sets of the program data indicated by a set of the program information corresponding to the matching identifier,

and judges that, (i) when either one of a judgment result by the 1st judging subunit and a judgment result by the 2nd judging subunit is negative, the requisition does not satisfy the access condition, and (ii) when both the judgment results are positive, the requisition satisfies the access condition.

30. The record carrier of Claim 24, wherein

the access condition includes (i) an identifier list including one or more identifiers which respectively identify one or more devices authorized to access the storage unit, and (ii) a biometrics list including one or more sets of biometric information for respectively identifying one or more users authorized to access the storage unit,

the requisition includes a requiring device identifier for identifying the terminal device and operator biometric information indicating biometric information of an operator of the terminal device; and

the judging unit includes:

a 1st judging subunit operable to judge whether or not an identifier matching the requiring device identifier is included in the identifier list; and

5 a 2nd judging subunit operable to judge, when the 1st judging subunit judges that the matching identifier is included, whether or not a set of the biometric information corresponding to the operator biometric information is included in the biometrics list,

10 and judges that, (i) when either one of a judgment result by the 1st judging subunit and a judgment result by the 2nd judging subunit is negative, the requisition does not satisfy the access condition, and (ii) when both the judgment results are positive, the requisition satisfies the access condition.

15

31. The record carrier of Claim 24, wherein

the access condition includes (i) an identifier list including one or more identifiers which respectively identify one or more devices authorized to access the storage unit, and (ii)
20 a password list including one or more sets of password information respectively specified by one or more users authorized to access the storage unit,

the requisition includes a requiring device identifier for identifying the terminal device and an entry password entered by
25 an operator of the terminal device, and

the judging unit includes:

a 1st judging subunit operable to judge whether or not an identifier matching the requiring device identifier is included in the identifier list; and

a 2nd judging subunit operable to judge whether or not a password indicated by a set of password information corresponding to the entry password is included in the password list,

and judges that, (i) when either one of a judgment result by the 1st judging subunit and a judgment result by the 2nd judging subunit is negative, the requisition does not satisfy the access condition, and (ii) when both the judgment results are positive, the requisition satisfies the access condition.

32. The record carrier of Claim 23, wherein

the acquisition unit acquires, each time when the requisition receiving unit receives the requisition, the access condition from the access condition management server.

33. The record carrier of Claim 23, wherein

the acquisition unit acquires the access condition from the access condition management server at predetermined time intervals.

34. The record carrier of Claim 23, wherein

the acquisition unit acquires, when it is detected that the record carrier is attached to a terminal device, the access condition from the access condition management server.

35. A data protection system comprising:

a record carrier including:

a storage unit,

a requisition receiving unit operable to receive, from

5 a terminal device having the record carrier attached thereto, a requisition for access to the storage unit,

an access condition storage unit operable to store an access condition indicating whether or not the terminal device is authorized to access the storage unit,

10 a judging unit operable to judge whether or not the requisition satisfies the access condition, and

a prevention unit operable to prevent the access to the storage unit when the judging unit judges the requisition does not satisfy the access condition; and

15 a terminal device including:

a record carrier interface operable to attach the record carrier thereto,

an access requisition generation unit operable to generate the requisition of the record carrier to the storage unit,

20 and

an access requisition output unit operable to output, to the record carrier, the generated requisition for access.

~~36. The data protection system of Claim 35, further comprising:~~

25 an access condition registration server operable to register the access condition with the access condition storage unit of the

record carrier via the terminal device having the record carrier attached thereto.

37.A data protection system comprising:

- 5 a record carrier including,
 - a storage unit,
 - a requisition receiving unit operable to receive, from a terminal device having the record carrier attached thereto, a requisition for access to the storage unit,
- 10 an access condition storage unit operable to store an access condition indicating whether or not the terminal device is authorized to access the storage unit,
 - a judging unit operable to judge whether or not the requisition satisfies the access condition, and
- 15 a prevention unit operable to prevent the access to the storage unit when the judging unit judges the requisition does not satisfy the access condition;
- a terminal device including,
 - a record carrier interface operable to attach the record
- 20 carrier thereto,
 - an access requisition generation unit operable to generate the requisition of the record carrier to the storage unit, and
 - an access requisition output unit operable to output, to
- 25 the record carrier, the generated requisition for access; and

an access condition management server connected, via a network, with the terminal device having the record carrier attached thereto, including,

an access condition storage unit operable to store the
5 access condition, and

an access condition transmission unit operable to transmit the access condition to the record carrier via the terminal device having the record carrier attached thereto.

10 38.A data protection method used by a record carrier including a storage unit and an access condition storage unit, comprising the steps of:

(a) receiving, from a terminal device having the record carrier attached thereto, a requisition for access to the storage
15 unit;

(b) acquiring, from the access condition storage unit, an access condition indicating whether or not the terminal device is authorized to access the storage unit;

(c) judging whether, or not the requisition satisfies the
20 access condition; and

(d) preventing the access to the storage unit when the step (c) judges that the requisition does not satisfy the access condition.

25 39.A data protection program used by a record carrier including

a storage unit and an access condition storage unit, comprising the steps of:

(a) receiving, from a terminal device having the record carrier attached thereto, a requisition for access to the storage
5 unit;

(b) acquiring, from the access condition storage unit, an access condition indicating whether or not the terminal device is authorized to access the storage unit;

(c) judging whether or not the requisition satisfies the
10 access condition; and

(d) preventing the access to the storage unit when the step (c) judges that the requisition does not satisfy the access condition.

15 40. A data protection method used by a record carrier including a storage unit, comprising the steps of:

(a) receiving, from a terminal device having the record carrier attached thereto, a requisition for access to the storage unit;

20 (b) communicating with an access condition management server connected via a network;

(c) acquiring from the access condition management server, as a result of the step (b), an access condition indicating whether or not the terminal device is authorized to access the storage unit;

25 (d) judging whether or not the requisition satisfies the

access condition; and

(e) preventing the access to the storage unit when the step (d) judges that the requisition does not satisfy the access condition.

5

41. A data protection program used by a record carrier including a storage unit, comprising the steps of:

(a) receiving, from a terminal device having the record carrier attached thereto, a requisition for access to the storage unit;

(b) communicating with an access condition management server connected via a network;

(c) acquiring from the access condition management server, as a result of the step (b), an access condition indicating whether or not the terminal device is authorized to access the storage unit;

(d) judging whether or not the requisition satisfies the access condition; and

(e) preventing the access to the storage unit when the step (d) judges that the requisition does not satisfy the access condition.